



(51) Internationale Patentklassifikation <sup>6</sup> :  G07D 7/00	A1	(11) Internationale Veröffentlichungsnummer: WO 96/29683  (43) Internationales Veröffentlichungsdatum: 26. September 1996 (26.09.96)
(21) Internationales Aktenzeichen: PCT/EP96/01178  (22) Internationales Anmeldedatum: 19. März 1996 (19.03.96)  (30) Prioritätsdaten: 195 10 626.1 23. März 1995 (23.03.95) DE		(81) Bestimmungsstaaten: CN, JP, RU, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(71) Anmelder ( <i>für alle Bestimmungsstaaten ausser US</i> ): GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).  (72) Erfinder; und (75) Erfinder/Anmelder ( <i>nur für US</i> ): ALBERT, Bodo [DE/DE]; Pfingstrosenstrasse 27A, D-81377 München (DE). BUNTSCHICK, Wilhelm [DE/DE]; Wiesenstrasse 21, D-82515 Wolfratshausen (DE).  (74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzererstrasse 106, D-80797 München (DE).		<b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>

(54) Title: METHOD OF VERIFYING THE INTEGRITY OF DATA STORED ON A PROCESSING FACILITY USED FOR PROCESSING SHEET-LIKE ARTICLES SUCH AS BANK NOTES OR BILLS

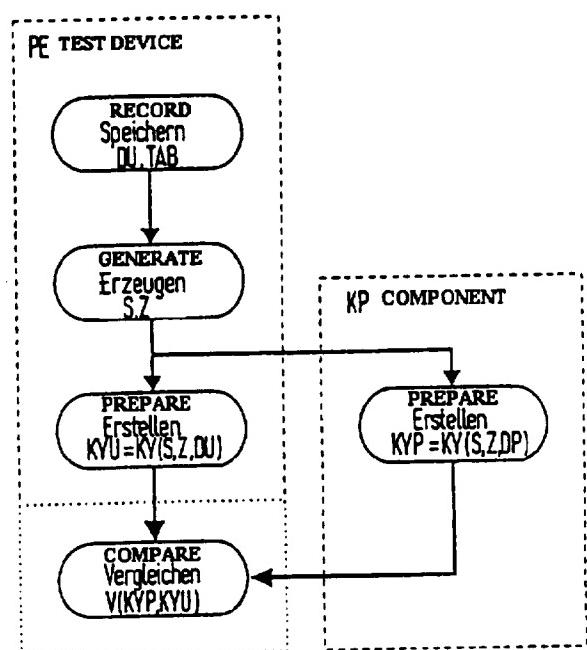
(54) Bezeichnung: VERFAHREN ZUR PRÜFUNG DER UNVERSEHRTHEIT VON GESPEICHERTEN DATEN AUF EINER VERARBEITUNGSANLAGE FÜR BLATTGUT, WIE Z.B. BANKNOTEN ODER WERTPAPIERE

#### (57) Abstract

In order to verify the integrity of stored data, intact data corresponding to the data to be tested relating to a component of the processing facility in a particular operating state and in an intact state are recorded on a test device. In order to check the integrity of the data to be tested on a component, a key which is different to those of preceding tests is produced in the test device for each test. By using this key and applying a cryptographic algorithm, two encrypted patterns are produced. One of these is derived from the data to be tested relating to the component in the processing facility on which the data to be tested are recorded. The other is derived by the test device from the intact data. The two encrypted data sequences are then compared; if they match, the tested data also match the intact data and contain no unwanted changes.

#### (57) Zusammenfassung

Zur Prüfung der Unversehrtheit von gespeicherten Daten werden zunächst auf einer Prüfeinrichtung unversehrte Daten gespeichert, die den zu prüfenden Daten einer Komponente der Verarbeitungsanlage in einem bestimmten Betriebszustand der Verarbeitungsanlage im unversehrten Zustand entsprechen. Zur Überprüfung der Unversehrtheit der zu prüfenden Daten auf einer Komponente wird für jede Prüfung ein Schlüssel in der Prüfeinrichtung erzeugt, der von denen vorheriger Prüfungen verschieden ist. Unter Verwendung dieses Schlüssels und mittels eines kryptografischen Algorithmus werden zwei Chiffren erstellt. Das eine Chiffren wird aus den zu prüfenden Daten von der Komponente der Verarbeitungsanlage erstellt, auf der die zu prüfenden Daten gespeichert sind. Das andere Chiffren wird von der Prüfeinrichtung aus den unversehrten Daten erstellt. Danach werden die beiden Chiffren miteinander verglichen. Entsprechen die Chiffren einander, so entsprechen auch die zu prüfenden Daten den unversehrten Daten und weisen somit keinerlei unerwünschte Veränderungen auf.



***LEDIGLICH ZUR INFORMATION***

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

Verfahren zur Prüfung der Unversehrtheit von gespeicherten Daten auf einer Verarbeitungsanlage für Blattgut, wie z. B. Banknoten oder Wertpapiere

- 5 Die Erfindung betrifft ein Verfahren zur Prüfung der Unversehrtheit von gespeicherten Daten auf einer Verarbeitungsanlage für Blattgut, wie z. B. Banknoten oder Wertpapiere.
- 10 Eine solche Verarbeitungsanlage ist im allgemeinen aus mehreren Komponenten aufgebaut. Jede dieser Komponenten erfüllt bestimmte Aufgaben bei der Bearbeitung des Blattguts. Die Verarbeitungsanlage weist als eine Komponente eine Steuereinrichtung auf, die den anderen Komponenten übergeordnet ist. Die Steuereinrichtung steuert die einzelnen Vorgänge der Verarbeitungsanlage. Die anderen Komponenten sind als Module ausgeführt, die die eigentliche Verarbeitung des Blattguts durchführen. Mögliche Verarbeitungsvorgänge einzelner Module sind z. B.
- 15 Vereinzeln des Blattgutes aus einem Stapel, Prüfen des Blattgutes auf Zustand oder Echtheit, Transport des Blattgutes, Stapeln oder Vernichten des Blattgutes.
- 20

In den Komponenten der Verarbeitungsanlage können Speicher vorgesehen sein, in denen Daten gespeichert werden, die zum Betrieb der Verarbeitungsanlage notwendig sind. Die Daten können beispielsweise Steuerungsbefehle, Programme, Ergebnisdaten oder Referenzdaten sein. Die einzelnen Komponenten der Verarbeitungsanlage sind untereinander so verbunden, daß zwischen ihnen Daten übertragen werden können.

Die Verarbeitungsanlage kann in verschiedenen Betriebszuständen betrieben werden. Die Betriebszustände können beispielsweise vom Bediener durch die Eingabe bestimmter Parameter festgelegt werden. Solche Parameter können die Anzahl der zu prüfenden Blätter, die Denomination bei Banknoten, die Art oder die Güte bestimmter Prüfkriterien oder ähnliche Angaben sein.

- 2 -

Aus der DE-PS 27 60 453 ist eine solche Verarbeitungsanlage bekannt. Zur Speicherung von Daten besitzen sowohl die Steuereinrichtung als auch einzelne Module jeweils einen eigenen Speicher, in dem Daten gespeichert sind, die zum Betrieb der Verarbeitungsanlage notwendig sind. Der Datenaustausch zwischen der Steuereinrichtung und den Modulen wird über einen Zentralspeicher durchgeführt, auf den sowohl die Module als auch die Steuereinrichtung zugreifen können. Zusätzlich sind die Module zum Datenaustausch noch direkt miteinander verbunden.

Die DE-OS 33 47 607 zeigt eine Verarbeitungsanlage, bei der zur optischen Prüfung des Blattguts mehrere gleichartige Module verwendet werden. Hier besitzen sowohl die Steuereinrichtung als auch die einzelnen Module einen eigenen Speicher zur Speicherung von Daten. Die einzelnen Module sind untereinander sowie mit der Steuereinrichtung über einen Datenbus verbunden. Zusätzlich ist an den Datenbus ein übergeordneter Speicher angeschlossen, auf den alle Komponenten der Verarbeitungsanlage zugreifen können.

Generell können bei Vorrichtungen der genannten Art unerwünschte Änderungen an den auf der Verarbeitungsanlage gespeicherten Daten stattfinden. Diese können entweder aufgrund von Störungen in der Verarbeitungsanlage, wie z. B. Datenübertragungsfehler oder Datenverlust, oder durch bewußte Manipulation der Daten in betrügerischer Absicht entstehen.

Bei den bekannten Vorrichtungen sind keine Maßnahmen vorgesehen, durch die unerwünschte Änderungen in den auf der Verarbeitungsanlage gespeicherten Daten festgestellt werden können.

Ausgehend davon liegt der Erfindung die Aufgabe zugrunde, ein Verfahren vorzuschlagen, bei dem die auf einer Verarbeitungsanlage für Blattgut gespeicherten Daten auf ihre Unversehrtheit geprüft werden, um Änderungen an diesen Daten feststellen zu können.

Diese Aufgabe wird durch die Merkmale des Hauptanspruchs gelöst.

- 10 Der Grundgedanke der Erfindung besteht im wesentlichen darin, zunächst auf einer Prüfeinrichtung unversehrte Daten zu speichern, die den zu prüfenden Daten einer Komponente der Verarbeitungsanlage in einem bestimmten Betriebszustand der Verarbeitungsanlage im unversehrten Zustand entsprechen. Zur Überprüfung der Unversehrtheit der zu prüfenden Daten auf der Komponente wird für jede Prüfung ein Schlüssel in der Prüfeinrichtung erzeugt, der von denen vorheriger Prüfungen verschieden ist. Unter Verwendung dieses Schlüssels und mittels eines kryptografischen Algorithmus werden zwei Chiffrate erstellt. Das eine Chiffrat wird aus den zu prüfenden Daten von der Komponente der Verarbeitungsanlage erstellt, auf der die zu prüfenden Daten gespeichert sind. Das andere Chiffrat wird von der Prüfeinrichtung aus den unversehrten Daten erstellt. Danach werden die beiden Chiffrate miteinander verglichen. Entsprechen die Chiffrate einander, so entsprechen auch die zu prüfenden Daten den unversehrten Daten und weisen somit keinerlei unerwünschte Veränderungen auf.
- 20
- 25
- 30
- 35 Ein Vorteil dieses Verfahrens ist es, daß ein Chiffrat durch die Prüfeinrichtung und das andere durch die zu prüfende Komponente berechnet wird. Dadurch verteilt sich auch die zur Bildung der Chiffrate benötigte Rechenkapazität.

- 4 -

Ein weiterer Vorteil besteht darin, daß bei jeder Prüfung ein Schlüssel erzeugt wird, der von denen vorheriger Prüfungen verschieden ist. Dieser muß somit nicht geheimgehalten werden. Die Gefahr einer Aus-

5 spähung des Schlüssels ist nicht gegeben.

Optional können die Daten, aus denen die Chiffrate erstellt werden, bei jeder Prüfung durch Hinzufügen einer Zufallszahl dynamisiert werden. Die aus den dynamisierten Daten erstellten Chiffrate ändern sich dann auch,

10 wenn dieselben Daten mehrmals geprüft werden. Hierdurch kann eine betrügerische Manipulation der Prüfung durch Einspielen von Chiffren von früherer Prüfung verhindert werden.

15 Vorzugsweise wählt man bei der Erstellung der Chiffrate einen kryptografischen Algorithmus, der gleichzeitig zu einer Datenreduktion führt. Dadurch weisen die Chiffrate Datenmengen auf, die verglichen mit den Datenmengen der ursprünglichen Daten relativ gering sind. Aufgrund der 20 geringen Datenmengen dieser Chiffrate können sie einfach und schnell ausgetauscht und verglichen werden.

25 In einer Weiterbildung der Erfindung können auch die gespeicherten Daten mehrerer Komponenten der Verarbeitungsanlage in einem Arbeitsgang geprüft werden. Hierzu wird auf der Prüfeinrichtung eine Tabelle gespeichert, in der, abhängig vom Betriebszustand der Verarbeitungsanlage, gespeichert ist, welche der Komponenten zu prüfen sind, in welchen Speicherbereichen die zu prüfenden Daten der jeweiligen Komponenten gespeichert sind und in 30 welchen Speicherbereichen der Prüfeinrichtung die korrespondierenden und unversehrten Daten gespeichert sind. Mit Hilfe dieser Tabelle kann die Prüfeinrichtung die 35 zur Überprüfung der einzelnen Komponenten notwendigen

- 5 -

Chiffrate erstellen und mit denen von den jeweiligen Komponenten erzeugten Chiffrate vergleichen.

Weitere Merkmale der Erfindung ergeben sich aus den Unteransprüchen. Nachfolgend werden einige Ausführungsbeispiele der Erfindung anhand der Figuren beschrieben. Es zeigen:

- Fig. 1 Flußdiagramm einer ersten Ausführungsform der Erfindung,
- Fig. 2 Flußdiagramm zweier Ausführungsformen des kryptografischen Algorithmus,
- Fig. 3 Prinzipskizze der Verarbeitungsanlage,
- Fig. 4 erste Implementation der ersten Ausführungsform der Erfindung,
- Fig. 5 Prinzipskizze eines Systems aus Verarbeitungsanlage und Hilfseinrichtung,
- Fig. 6 zweite Implementation der ersten Ausführungsform der Erfindung,
- Fig. 7 Flußdiagramm einer zweiten Ausführungsform der Erfindung,
- Fig. 8 Prinzipskizze einer erweiterten Verarbeitungsanlage,
- Fig. 9 Implementation der zweiten Ausführungsform.

Fig. 1 zeigt ein Flußdiagramm einer ersten Ausführungsform der Erfindung. Zur Prüfung der Unversehrtheit von gespeicherten Daten auf einer Komponente KP einer Ver-

arbeitungsanlage für Blattgut durch eine Prüfeinrichtung PE werden zunächst unversehrte Daten DU auf der Prüfeinrichtung PE gespeichert. Diese unversehrten Daten DU entsprechen den zu prüfenden Daten DP auf der Komponente 5 KP der Verarbeitungsanlage in einem bestimmten Betriebszustand BZ der Verarbeitungsanlage im unversehrten Zustand.

Bei jeder Prüfung von gespeicherten Daten auf einer Komponente KP der Verarbeitungsanlage wird durch die Prüfeinrichtung PE ein Schlüssel S erzeugt, der bei jeder Prüfung der Unversehrtheit von Daten verschieden ist. Der Schlüssel S wird zur Erzeugung von Chiffrenmittels eines kryptografischen Algorithmus KY benutzt. Optional kann noch eine Zufallszahl Z von der Prüfeinrichtung PE erzeugt werden, die zur Dynamisierung der Daten DP bzw. DU benutzt wird.

Die zur Erstellung eines Chiffrets notwendigen Daten S bzw. Z werden dann von der Prüfeinrichtung PE zur zu prüfenden Komponente KP übertragen. Sowohl auf der Prüfeinrichtung PE als auch auf der zu prüfenden Komponente KP wird ein Chiffrat mittels eines kryptografischen Algorithmus KY und des Schlüssels S bzw. der Zufallszahl Z berechnet. Auf der Komponente KP der Verarbeitungsanlage wird ein Chiffrat KYP aus den zu prüfenden Daten DP erstellt. Ein Chiffrat KYU wird durch die Prüfeinrichtung PE aus den unversehrten Daten DU erstellt, wobei die unversehrten Daten DU den zu prüfenden Daten DP im unversehrten Zustand entsprechen.

Anschließend werden die Chiffrate KYU und KYP in einem Vergleich V verglichen. Hierzu wird das Chiffrat KYP von der zu prüfenden Komponente KP an die Prüfeinrichtung PE übertragen. Der Vergleich V kann beispielsweise direkt von der Prüfeinrichtung PE durchgeführt werden. Eine

weitere Möglichkeit des Vergleichs V besteht darin, so-  
wohl das Chiffrat KYU als auch das Chiffrat KYP in les-  
barer Form auszugeben und den Vergleich V der Chiffrate  
von einem Bediener BD der Verarbeitungsanlage durchfüh-  
5 ren zu lassen.

Sollen mehrere Komponenten in der Verarbeitungsanlage  
oder eine Komponente zu unterschiedlichen Betriebszu-  
ständen BZ der Verarbeitungsanlage oder eine Kombination  
10 dieser beiden Möglichkeiten geprüft werden, so kann op-  
tional eine Tabelle TAB in der Prüfeinrichtung gespei-  
chert werden. In dieser Tabelle TAB ist abhängig von  
möglichen Betriebszuständen BZ der Verarbeitungsanlage  
gespeichert, welche Komponenten zu prüfen sind, in wel-  
15 chen Speicherbereichen SP die zu prüfenden Daten DP der  
jeweiligen Komponente gespeichert sind und welche Spei-  
cherbereiche SU der Prüfeinrichtung PE die korrespon-  
dierenden und unversehrten Daten DU gespeichert sind.  
Zusätzlich werden in der Prüfeinrichtung PE alle unver-  
20 sehrten Daten DU gespeichert, die abhängig von den mög-  
lichen Betriebszuständen BZ der Verarbeitungsanlage in  
der Tabelle TAB auftreten.

Die Speicherbereiche SP bzw. SU können beispielsweise  
25 unter Verwendung direkter physikalischer Speicher-  
adressen oder logischer Namen definiert werden. Die Ver-  
wendung direkter physikalischer Speicheradressen wird im  
allgemeinen bei Halbleiterspeichern verwendet, wie z. B.  
RAM, ROM, EPROM, EEPROM oder ähnlichem. Ein Speicher-  
30 bereich kann hier beispielsweise durch die Angabe einer  
Startadresse und einer Endadresse im Speicher oder durch  
die Angabe einer Startadresse und der Länge des Spei-  
cherbereichs im Speicher festgelegt werden. Bei Massen-  
speichern, wie z. B. Festplattenlaufwerken, Disketten-  
35 laufwerken, Streamer, CD-ROM-Laufwerke oder ähnlichem,

werden im allgemeinen logische Namen (Dateinamen) zur Festlegung bestimmter Speicherbereiche verwendet.

Fig. 2a zeigt eine Ausführungsform des kryptografischen Algorithmus KY. Die zu verschlüsselnden Daten DU bzw. DP können hier vor Durchführung des eigentlichen kryptografischen Algorithmus KY durch Hinzufügen einer Zufallszahl Z dynamisiert werden. Diese Dynamisierung kann durchgeführt werden, um auch bei ansonsten gleichem kryptografischen Algorithmus KY unterschiedliche Kryptogramme KYU bzw. KYP zu erhalten. Durch diese Vorgehensweise kann verhindert werden, daß in Folge einer betrügerischen Manipulation der Verarbeitungsanlage Chiffre alter Überprüfungen ausgespäht werden und diese dann zur Vortäuschung einer korrekten Überprüfung in die Verarbeitungsanlage eingespielt werden.

Die optional durch die Zufallszahl Z dynamisierten Daten DU bzw. DP werden dann mittels eines Komprimierungsverfahrens KV komprimiert. Die so erhaltenen komprimierten Daten KD werden dann mittels eines Verschlüsselungsverfahrens VV unter der Verwendung des Schlüssels S verschlüsselt. Ergebnis dieses Verschlüsselungsverfahrens VV ist dann das gewünschte Chiffra KYU bzw. KYP.

Allgemein können zur Komprimierung und zur Verschlüsselung alle gängigen Verfahren benutzt werden. Bekannte Komprimierungsverfahren sind beispielsweise Hashfunktionen. Als Verschlüsselungsverfahren VV lassen sich beispielsweise der Data Encryption Standard (DES) oder Public-Key-Verfahren, wie der RSA-Algorithmus, verwenden.

Die Fig. 2b zeigt eine weitere Ausführungsform des kryptografischen Algorithmus KY. Hier wird den zu verschlüsselnden Daten DU bzw. DP zunächst der Schlüssel S

- 9 -

hinzugefügt und danach mittels eines Komprimierungsverfahrens KV direkt zum Chiffrat KYU bzw. KYP komprimiert. Generell sind auch andere Ausführungsformen des kryptografischen Algorithmus KY möglich.

5

Fig. 3 zeigt eine Prinzipskizze einer Verarbeitungsanlage für Blattgut. Sie ist hier aus drei Komponenten 10, 20, 30 aufgebaut, wobei die einzelnen Komponenten über eine Datenleitung 100 verbunden sind. Die Steuereinrichtung 10 ist eine den anderen Komponenten übergeordnete Komponente und dient zur Steuerung der einzelnen Verarbeitungsvorgänge. Sie besitzt unter anderem einen Prozessor 11, der auf Halbleiterspeicher 12 und Massenspeicher 13 zugreifen kann.

15

Die Halbleiterspeicher 12 können beispielsweise aus flüchtigen RAM- oder nichtflüchtigen ROM, EPROM, EEPROM oder ähnlichen Speichern bestehen. Im allgemeinen wird der flüchtige RAM vom Prozessor 11 während der Ausführung eines Programms genutzt. Die nichtflüchtigen Speicher enthalten Daten, die zum Betrieb der Verarbeitungsanlage notwendig sind. Speicherbereiche dieser Halbleiterspeicher 12 werden im allgemeinen unter der Verwendung direkter physikalischer Speicheradressen festgelegt.

20

25

Die Massenspeicher 13 dienen zur Speicherung von größeren Datenmengen und können beispielsweise durch Festplattenlaufwerke, Diskettenlaufwerke, CD-ROM-Laufwerke oder ähnlichem realisiert werden. In den Massenspeichern 13 werden Daten gespeichert, die für den Betrieb der Verarbeitungsanlage notwendig sind. Speicherbereiche des Massenspeicher 13 werden im allgemeinen unter der Verwendung logischer Namen festgelegt.

30

35

- 10 -

Als weitere Komponenten der Verarbeitungsanlage sind hier zwei Module 20 und 30 gezeigt. Diese weisen zwar ein gleiches Blockschaltbild auf, führen aber innerhalb der Verarbeitungsanlage unterschiedliche Aufgaben bei der Bearbeitung des Blattguts aus. Die Anzahl der Module wurde hier lediglich aus Gründen der Übersichtlichkeit auf zwei beschränkt.

Jedes dieser Module 20 bzw. 30 besitzt analog zur Steuereinrichtung 10 einen Prozessor 21 bzw. 31, Halbleiter-Speicher 22 bzw. 32 und Massenspeicher 23 bzw. 33. Die in den Speichern 22, 23, 32, 33 gespeicherten Daten dienen zum Betrieb des jeweiligen Moduls.

Generell sind die in den Speichern 12, 13, 22, 23, 32, 33 gespeicherten Daten unterschiedlich und hängen im allgemeinen vom Betriebszustand BZ der Verarbeitungsanlage und der Funktion der Komponente ab.

In einem in Fig. 4 gezeigten Flußdiagramm einer ersten Implementation der ersten Ausführungsform werden die Aufgaben der Prüfeinrichtung PE von der Steuereinrichtung 10 übernommen. Die unverührten Daten DU, die den in den Speichern 12, 13, 22, 23, 32, 33 gespeicherten zu prüfenden Daten DP im unversehrten Zustand entsprechen, werden gemäß Fig. 3 im Massenspeicher 13 der Steuereinrichtung 10 in den entsprechenden Speicherbereichen D12, D13, D22, D23, D32 und D33 gespeichert. Zusätzlich wird eine entsprechende Tabelle TAB zur Prüfung mehrerer Komponenten der Verarbeitungsanlage auf dem Massenspeicher 13 gespeichert. Die zur Prüfung notwendigen Chiffrate KYU werden von der Steuereinrichtung 10 erstellt. Die entsprechenden Chiffrate KYP werden auf den zu prüfenden Komponenten erstellt. Die zu prüfenden Komponenten KP können hier beispielsweise die Module 20 oder 30 sein, aber auch die Steuereinrichtung 10 selbst.

Der Vergleich V der erstellten Chiffrate KYP und KYU wird dann entweder von der Steuereinrichtung 10 durchgeführt oder diese werden von der Steuereinrichtung 10 in lesbbarer Form ausgegeben, so daß der Vergleich V von 5 einem Bediener der Verarbeitungsanlage durchgeführt werden kann.

Fig. 5 zeigt eine Prinzipskizze einer Verarbeitungsanlage, bei der eine zusätzliche Hilfseinrichtung 40 vorgesehen wird. Die Hilfseinrichtung 40 kann beispielsweise 10 ein Personal-Computer sein, der räumlich von der Verarbeitungsanlage getrennt sein kann. Auch die Hilfseinrichtung 40 besitzt einen Prozessor 41, Halbleiterspeicher 42 und Massenspeicher 43. Da im folgenden die 15 Hilfseinrichtung 40 die Aufgaben der Prüfeinrichtung PE übernehmen soll, sind die zur Prüfung notwendigen unverührten Daten DU bzw. die Tabelle TAB auf den Massenspeicher 43 der Hilfseinrichtung 40 gespeichert.

- 20 Der zur Durchführung der Prüfung notwendige Datenaustausch zwischen der Hilfseinrichtung 40 und der Verarbeitungsanlage kann auf unterschiedliche Art und Weise erfolgen. Eine Möglichkeit besteht darin, daß die Daten von der Hilfseinrichtung 40 auf einen tragbaren Datenträger 101 geschrieben werden, die dann in die Steuereinrichtung 10 eingegeben wird. Als tragbare Datenträger 25 101 können beispielweise Chipkarten oder Disketten eingesetzt werden.
- 30 Eine weitere Möglichkeit besteht darin, eine Datenleitung 102 vorzusehen, die einen Datenaustausch zwischen der Steuereinrichtung 10 und der Hilfseinrichtung 40 ermöglicht. Abhängig von den räumlichen Gegebenheiten kann diese Datenleitung 102 aus einer direkten Verbindung der beiden Komponenten oder aus einem Netzwerk 35 bestehen.

Weiterhin ist es möglich, die Hilfseinrichtung 40 direkt an die interne Datenleitung 100 der Verarbeitungsanlage anzuschließen. In diesem Fall kann die Hilfseinrichtung 40 als Komponente der Verarbeitungsanlage angesehen werden.

Fig. 6 zeigt ein Flußdiagramm einer zweiten Implementierung der ersten Ausführungsform auf einer Verarbeitungsanlage mit einer Hilfseinrichtung 40. Wie schon oben ausgeführt, werden die unversehrten Daten DU bzw. die Tabelle TAB auf der Hilfseinrichtung 40 gespeichert. Weiterhin wird der Schlüssel S bzw. die Zufallszahl Z auf der Hilfseinrichtung 40 erzeugt. Zur Prüfung der Unversehrtheit von gespeicherten Daten auf der Verarbeitungsanlage werden der Schlüssel S bzw. die Zufallszahl Z über eine der oben beschriebenen Verbindungen 101, 102, 103 zur Steuereinrichtung 10 übertragen.

Zur Prüfung der Unversehrtheit der Daten muß nun die Steuereinrichtung 10 in den zur Überprüfung notwendigen Betriebszustand BZ versetzt werden. Dies kann entweder durch eine Information erfolgen, die direkt durch den Bediener in die Steuereinrichtung 10 eingegeben wird oder durch eine entsprechende Information, die von der Hilfseinrichtung 40 an die Steuereinrichtung 10 übertragen wird. Abhängig von dieser Information versetzt die Steuereinrichtung 10 die Verarbeitungsanlage in den gewünschten Betriebszustand BZ.

Die zur Prüfung notwendigen Informationen, welche Komponenten zu prüfen sind und in welchen Speicherbereichen SP die zu prüfenden Daten DP der jeweiligen Komponenten 10, 20, 30 gespeichert sind, können von der Hilfseinrichtung 40 abhängig vom gewünschten Betriebszustand BZ aus der Tabelle TAB gelesen und an die Steuereinrichtung 10 übertragen werden.

Eine andere Möglichkeit besteht darin, eine Kopie der Tabelle TAB auf der Steuereinrichtung 10 zu speichern. Die Steuereinrichtung 10 kann dann die notwendigen Informationen abhängig vom eingestellten Betriebszustand 5 BZ direkt aus dem Duplikat der Tabelle TAB lesen.

Die Hilfseinrichtung 40 erstellt dann die notwendigen Chiffrate KYU, während die zum Vergleich notwendigen Chiffrate KYP auf den jeweiligen Komponenten 10, 20, 30 10 der Verarbeitungsanlage erstellt werden.

Zum Vergleich V der Chiffrate KYU und KYP können nun die Chiffrate KYU von der Hilfseinrichtung 40 zur Steuereinrichtung 10 übertragen und dort verglichen werden. Alternativ dazu ist es auch möglich, die Chiffrate KYU und die Chiffrate KYP von der Steuereinrichtung 10 in lesbbarer Form ausgeben zu lassen. Der Vergleich der Chiffrate kann dann vom Bediener der Verarbeitungsanlage durchgeführt werden.

Wird als Übertragungsmedium zwischen Hilfseinrichtung 40 und der Steuereinrichtung 10 der tragbare Datenträger 101 gewählt, so kann aus ökonomischen Gründen der Schlüssel S bzw. die Zufallszahl Z sowie die erstellten Chiffrate KYU in einem Arbeitsschritt auf den tragbaren 25 Datenträger 101 geschrieben und mit einem Mal zur Steuereinrichtung 10 übertragen werden.

Die Fig. 7 zeigt ein Flußdiagramm einer weiteren Ausführungsform der Erfindung. Werden gespeicherte Daten von mehreren Komponenten der Verarbeitungsanlage geprüft, so müssen auf der Prüfeinrichtung PE mehrere Chiffrate KYU erstellt werden. Zur Entlastung der Prüfeinrichtung PE wird in dieser Ausführungsform die Berechnung der Chiffrate auf eine zusätzliche Recheneinrichtung RE verlagert. Hierzu werden die unversehrten Daten DU und der 30 35

zur Berechnung der Chiffrate KYU notwendige Schlüssel S bzw. die Zufallszahl Z an die Recheneinrichtung RE übertragen. Diese erstellt dann die Chiffrate KYU aus den unversehrten Daten DU und überträgt die Chiffrate KYU 5 wieder an die Prüfeinrichtung PE. Die anderen Verfahrensschritte werden analog zur Beschreibung der ersten Ausführungsform durchgeführt.

Fig. 8 zeigt eine erweiterte Verarbeitungsanlage, bei 10 der zusätzlich eine Recheneinrichtung 50 vorgesehen ist. Auch diese weist einen Prozessor 51, Halbleiterspeicher 52 und Massenspeicher 53 auf. Die Recheneinrichtung 50 kann beispielsweise durch einen Personal-Computer realisiert werden. Die Recheneinrichtung 50 ist entweder über 15 eine Datenleitung 104 analog zur Datenleitung 102 oder durch eine Datenleitung 105 analog zur Datenleitung 103 mit der Verarbeitungsanlage verbunden.

Eine Verbindung zwischen der Recheneinrichtung 50 und 20 der Steuereinrichtung 10 über einen tragbaren Datenträger ist zwar prinzipiell möglich, bietet sich aber hier nicht an, da die unversehrten Daten DU vollständig von der Steuereinrichtung 10 an die Recheneinrichtung 50 übertragen werden müssen und es sich bei den unversehrten Daten DU um durchaus große Datenmengen handeln kann. 25

Die Fig. 9 zeigt ein Flußdiagramm einer Implementation 30 der zweiten Ausführungsform auf einer Verarbeitungsanlage mit Recheneinrichtung 50. Das Flußdiagramm unterscheidet sich von dem der ersten Implementation der ersten Ausführungsform in Fig. 4 lediglich darin, daß die Berechnung der Chiffrate KYU auf der Recheneinrichtung 50 durchgeführt wird und diese anschließend zur Steuereinrichtung 10 übertragen werden. Der Vergleich V der 35 Chiffrate KYP und KYU kann auch hier wiederum entweder direkt auf der Steuereinrichtung 10 oder nach Ausgabe

der Chiffrate in lesbarer Form vom Bediener der Verarbeitungsanlage durchgeführt werden.

Generell ist es möglich, die Erfindung auch auf hier  
5 nicht explizit beschriebene Ausführungsformen zu übertragen. Weiterhin ist es möglich, daß die in den Ausführungsformen genannten Speicher der einzelnen Komponenten lediglich einfach ausgeführt sind oder bei Bedarf auch teilweise entfallen können.

P a t e n t a n s p r ü c h e :

1. Verfahren zur Prüfung der Unversehrtheit von gespeicherten Daten in einer Verarbeitungsanlage für Blattgut,  
5 wie z.B. Banknoten oder Wertpapiere, durch eine Prüfeinrichtung, wobei die Verarbeitungsanlage mehrere Komponenten zur Bearbeitung des Blattguts aufweist und in verschiedenen Betriebszuständen betrieben werden kann, dadurch gekennzeichnet, daß die folgenden Schritte durchgeführt werden:  
10

- Speichern von unversehrten Daten (DU) in der Prüfeinrichtung (PE), wobei die unversehrten Daten (DU) den zu prüfenden Daten (DP) einer Komponente (KP) der Verarbeitungsanlage in einem bestimmten Betriebszustand (BZ) der Verarbeitungsanlage im unversehrten Zustand entsprechen;
- Erzeugen eines Schlüssels (S) durch die Prüfeinrichtung (PE), wobei der Schlüssel (S) bei jeder Prüfung der Unversehrtheit von Daten verschieden ist;
- Erstellen eines Chiffrats (KYP) durch eine Komponente (KP), deren Daten geprüft werden sollen, in einem bestimmten Betriebszustand (BZ) der Verarbeitungsanlage, wobei das Chiffrat (KYP) aus den zu prüfenden Daten (DP) der Komponente (KP) mittels eines kryptografischen Algorithmus (KY) und des Schlüssels (S) berechnet wird;
- Erstellen eines Chiffrats (KYU) durch die Prüfeinrichtung (PE), wobei das Chiffrat (KYU) aus den unversehrten Daten (DU) mittels des kryptografischen Algorithmus (KY) und des Schlüssels (S) berechnet wird;

- 17 -

- Vergleich (V) der Chiffrate (KYU, KYP).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Prüfung von gespeicherten Daten mehrerer Komponenten (10,20,30) der Verarbeitungsanlage eine Tabelle (TAB) in der Prüfeinrichtung (PE) gespeichert ist, in der, abhängig vom Betriebszustand (BZ) der Verarbeitungsanlage, die folgenden Daten gespeichert sind:

- 10
- welche der Komponenten (10,20,30) zu prüfen sind,
  - in welchen Speicherbereichen (SP) die zu prüfenden Daten (DP) der jeweiligen Komponente (10,20,30) gespeichert sind und
  - in welchen Speicherbereichen (SU) der Prüfeinrichtung (PE) die korrespondierenden unversehrten Daten (DU) gespeichert sind.

20

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß auf die Speicherbereiche (SP, SU) unter Verwendung direkter physikalischer Speicheradressen und/oder logischer Namen zugegriffen werden kann.

25

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Daten (DU, DP) vor der Ausführung des kryptografischen Algorithmus (KY) durch Hinzufügen einer Zufallszahl (Z) dynamisiert werden.

30

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der kryptografische Algorithmus (KY) die Daten (DU, DP) zunächst mittels eines Komprimierungsverfahrens (KV) komprimiert und dann die komprimierten Daten (KD) mittels eines Verschlüsselungsverfah-

35

rens (VV) unter Verwendung des Schlüssels (S) verschlüsselt.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Erstellung des Chiffrats (KYU)

- die unversehrten Daten (DU) und der Schlüssel (S) bzw. die Zufallszahl (Z) von der Prüfeinrichtung (PE) über eine Datenleitung (104, 105) an eine Recheneinrichtung (RE) übertragen werden,

- die Recheneinrichtung (RE) das Chiffrat (KYU) berechnet und

- die Recheneinrichtung (RE) das Chiffrat (KYU) über die Datenleitung (104, 105) an die Prüfeinrichtung (PE) überträgt.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Recheneinrichtung (RE) eine Komponente (50) der Verarbeitungsanlage ist.

8. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Recheneinrichtung (RE) eine externe Einrichtung ist.

9. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Prüfeinrichtung (PE) eine Komponente (10) der Verarbeitungsanlage ist.

10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Prüfeinrichtung (PE) eine externe Einrichtung (40) ist.

35 11. Verfahren nach Anspruch 10, dadurch gekenn-

zeichnet, daß zur Prüfung notwendige Daten zwischen der Verarbeitungsanlage und der externen Einrichtung (40) mittels eines tragbaren Datenträgers (101) übertragen werden.

5

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß zur Prüfung notwendige Daten zwischen der Verarbeitungsanlage und der externen Einrichtung (40) mittels einer Datenleitung (102, 103) übertragen werden.

10

13. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Vergleich (V) von der Prüfeinrichtung (PE) durchgeführt wird.

15

14. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Chiffrate (KYP, KYU) in lesbbarer Form ausgegeben werden und der Vergleich (V) von einem Bediener (BD) der Verarbeitungsanlage durchgeführt wird.

20

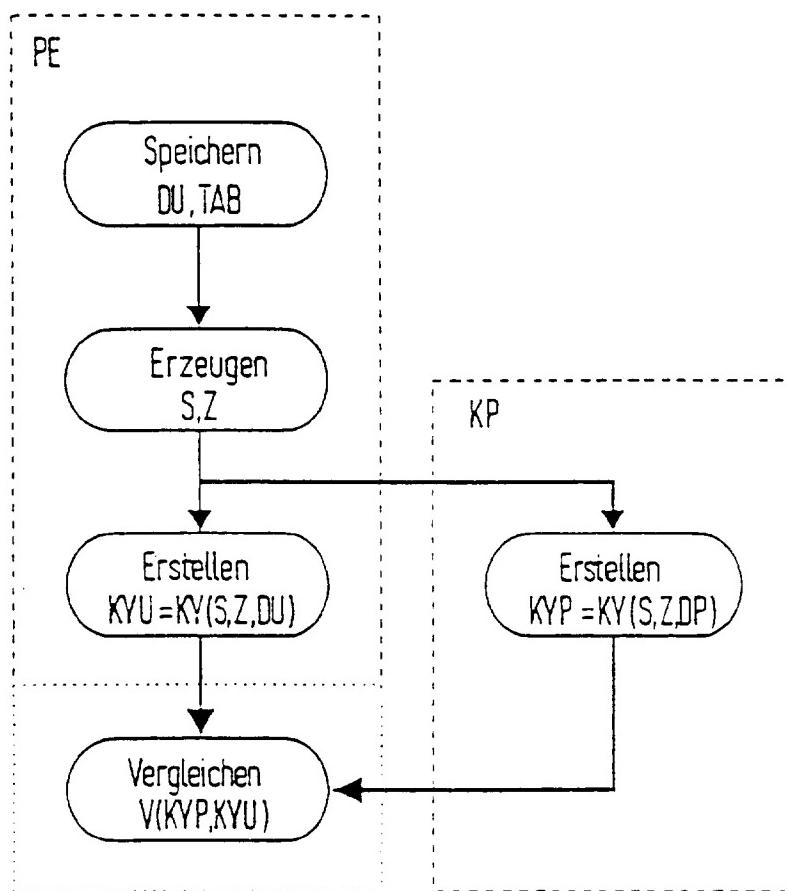


FIG.1

2/9

FIG.2a

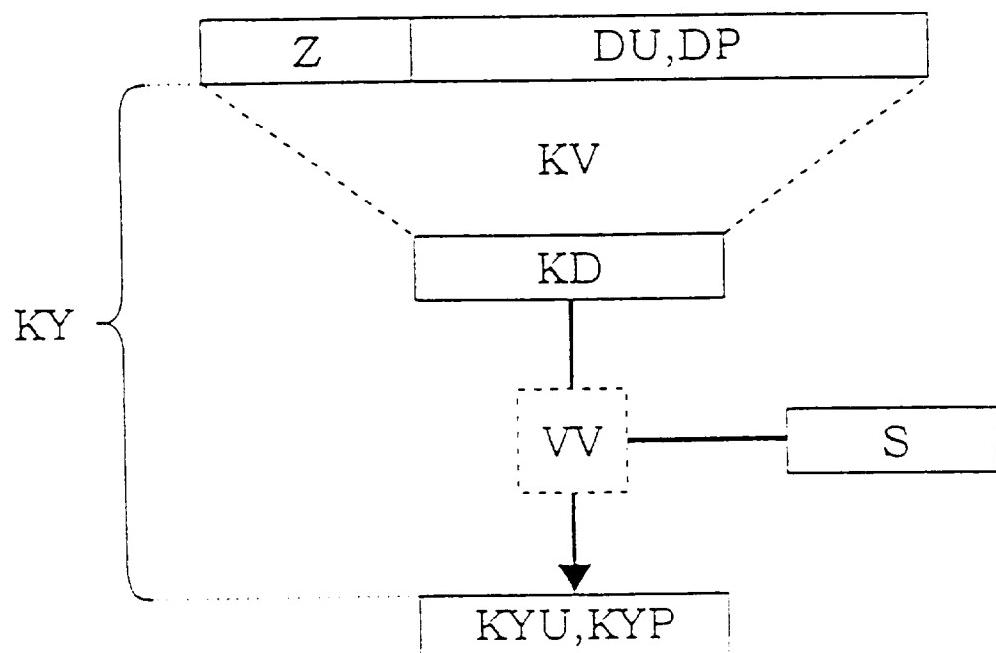
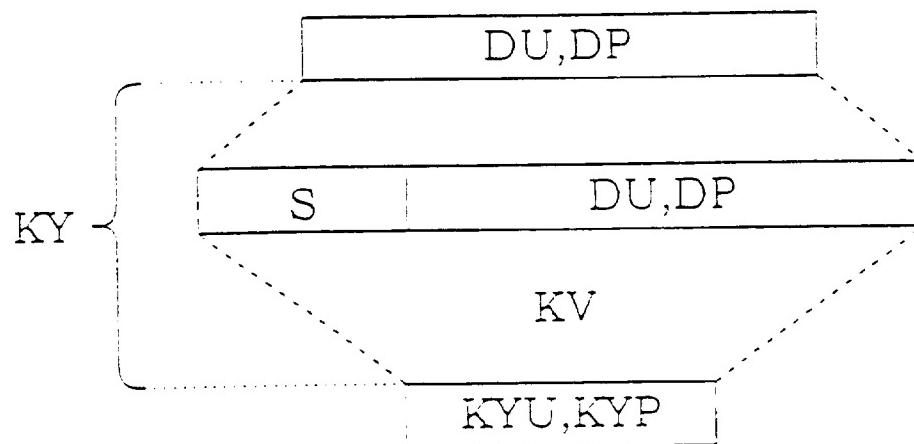
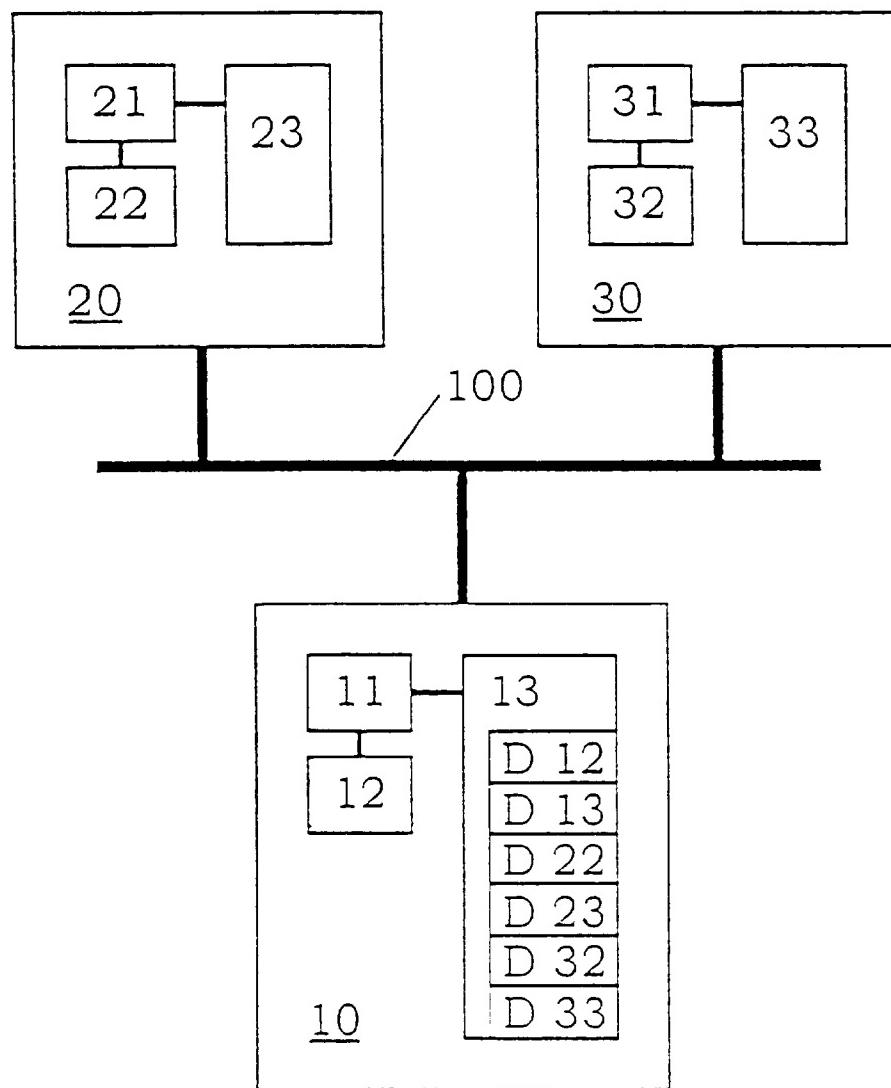


FIG.2b



3/9

FIG. 3



4/9

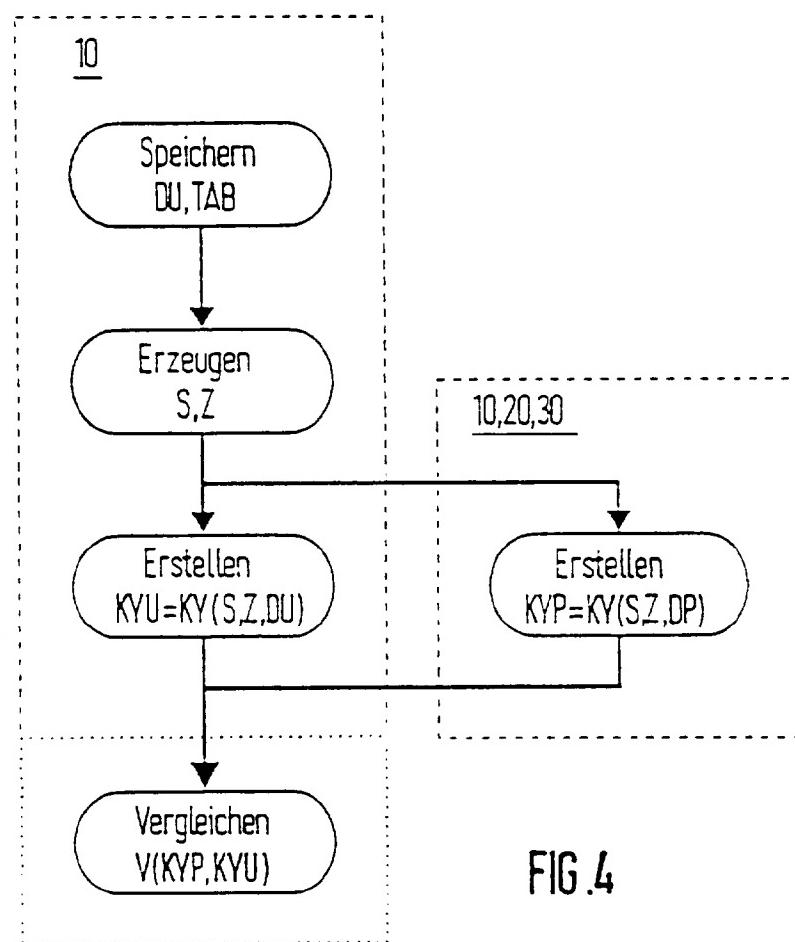
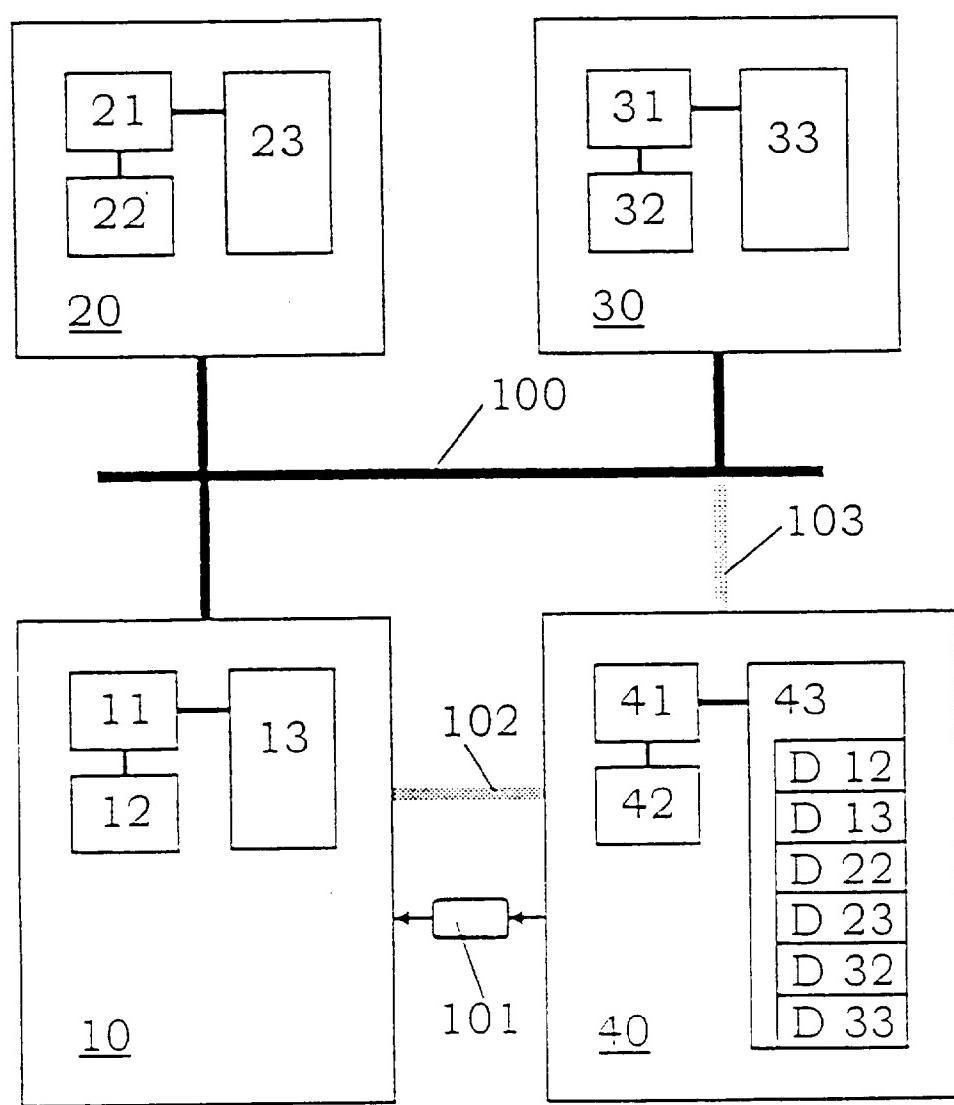


FIG.4

FIG.5



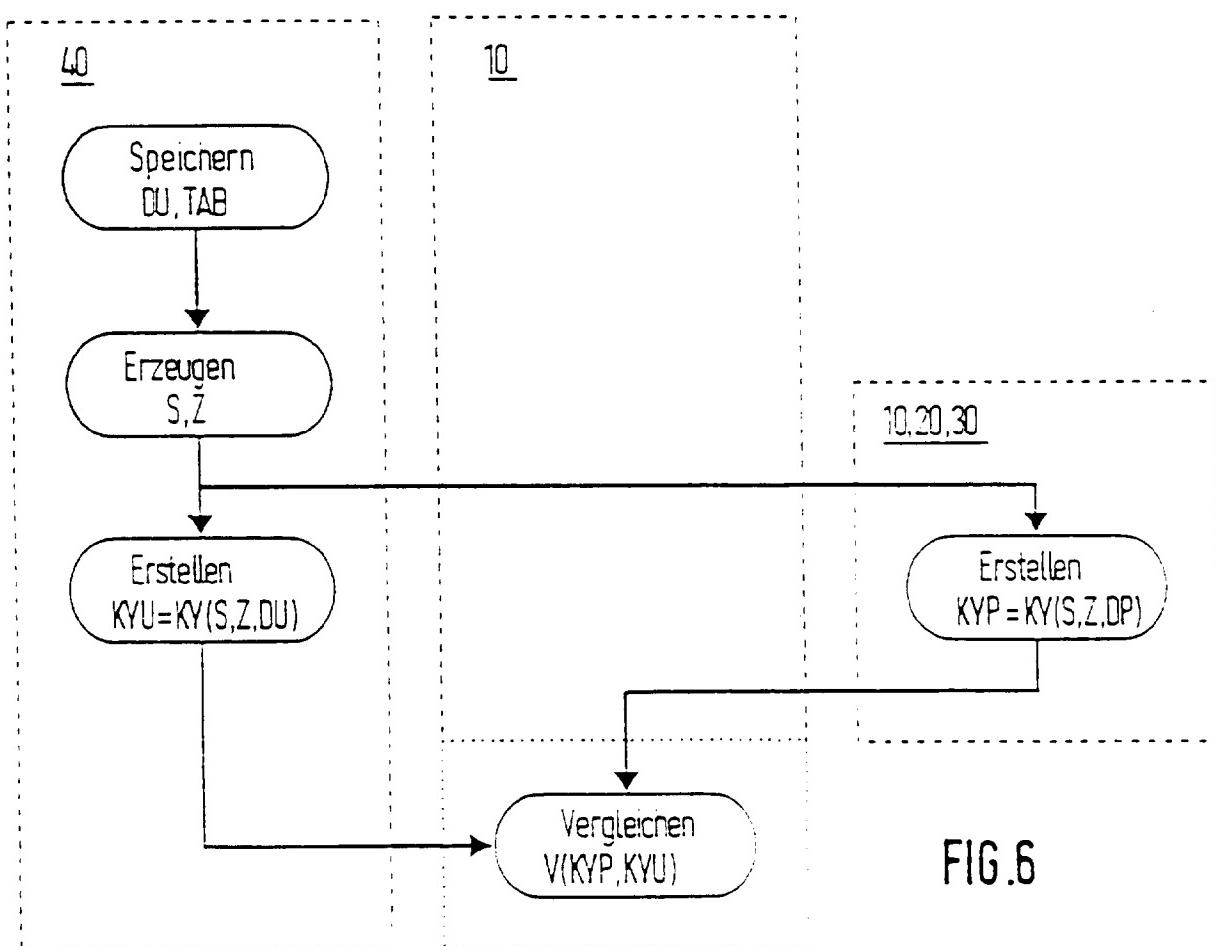


FIG.6

7/9

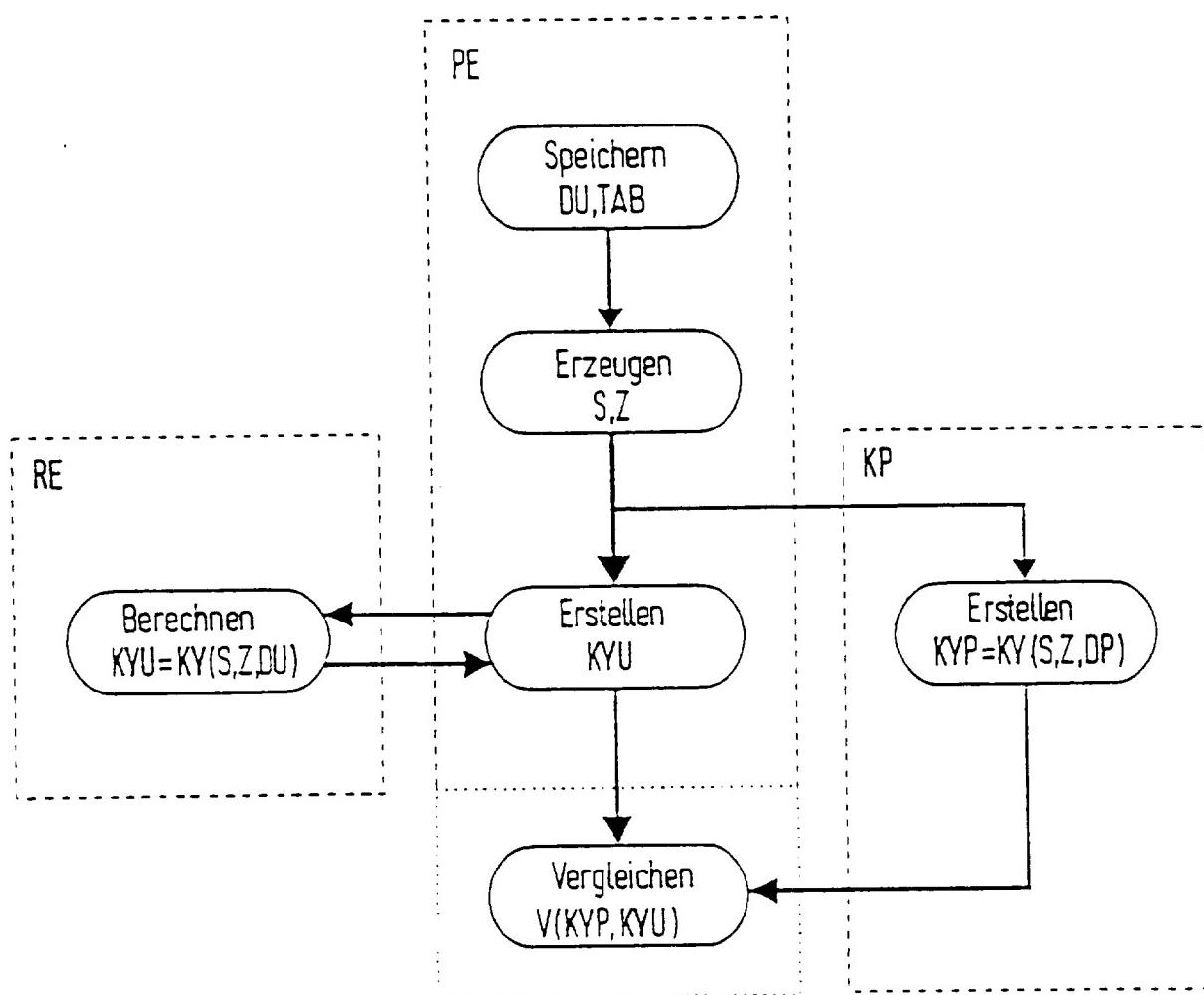
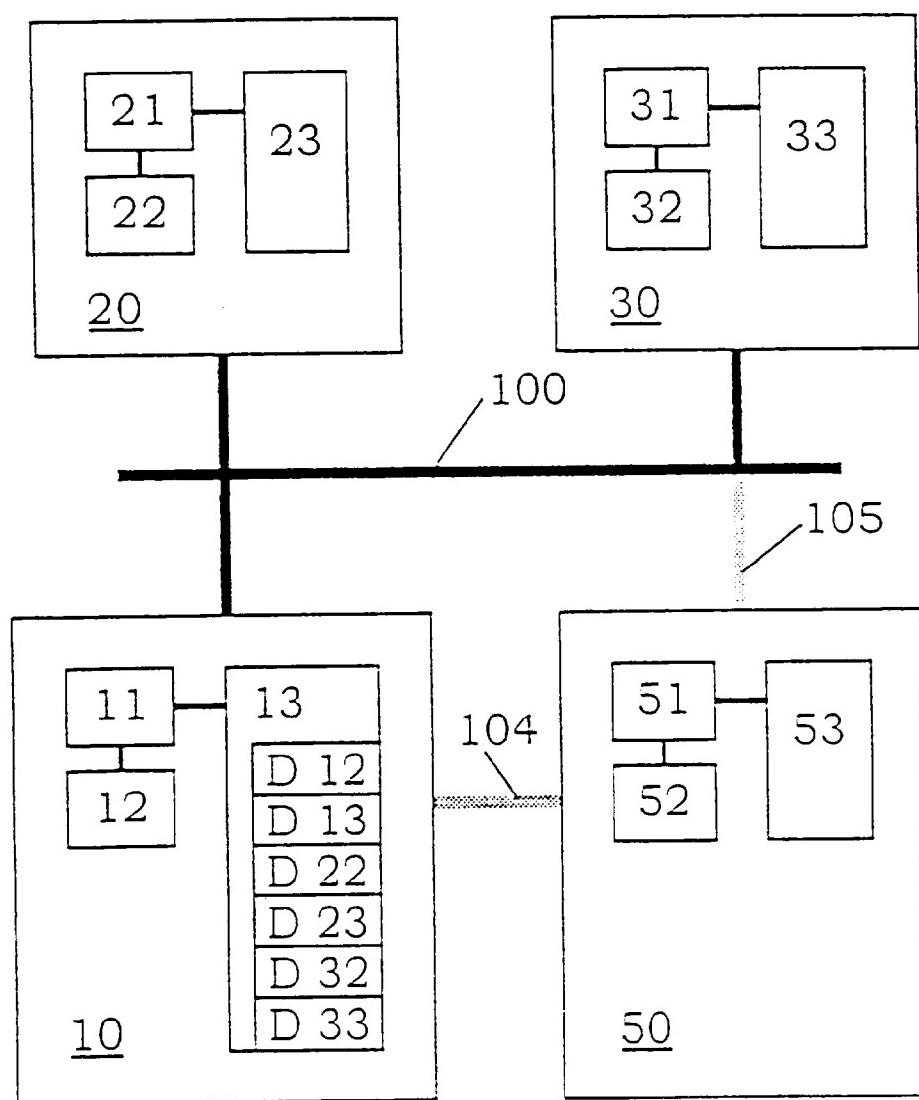


FIG.7

FIG.8



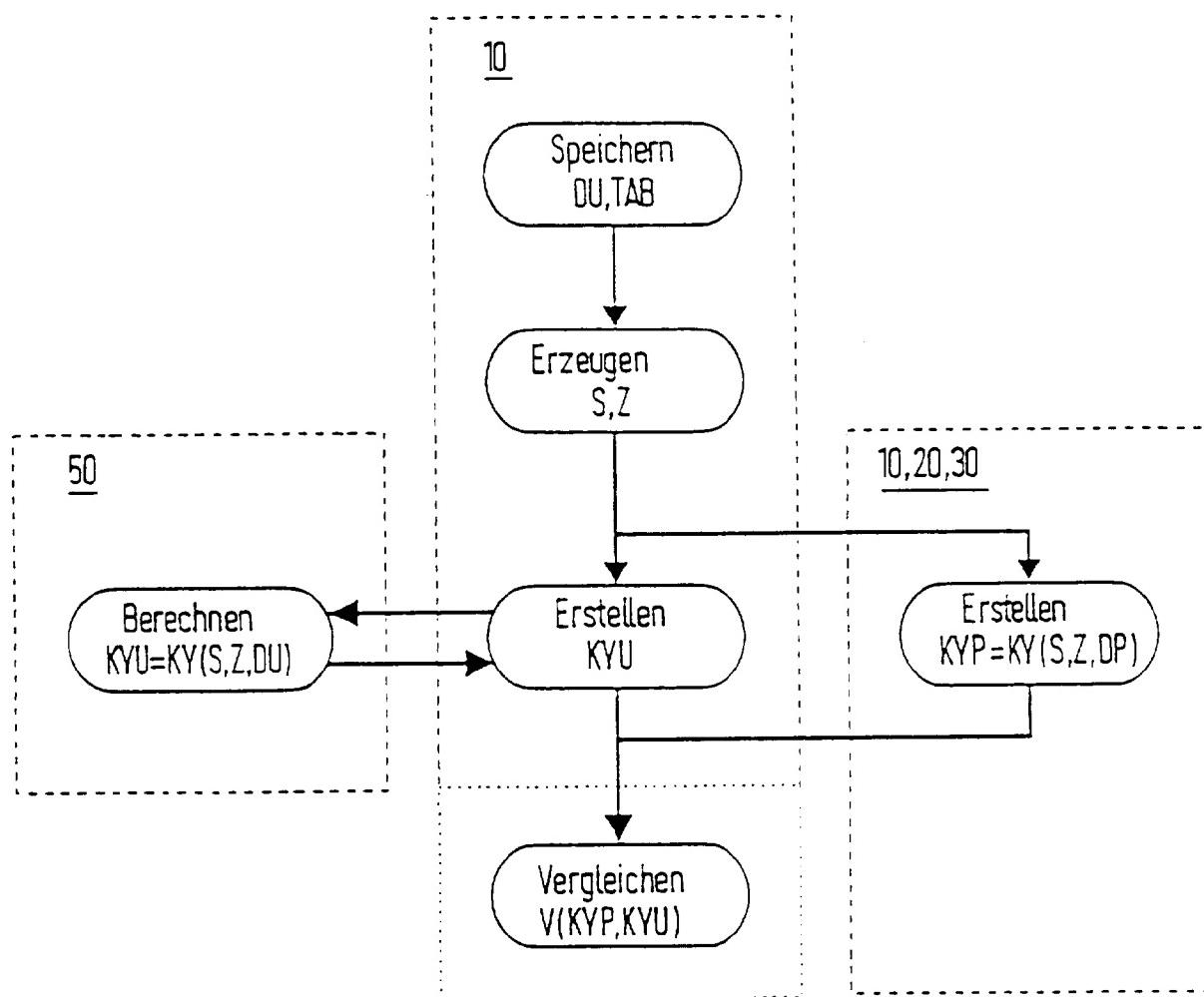


FIG.9

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP 96/01178

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 6 G07D7/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 358 849 (SERY JACQUES) 9 November 1982 see claim 1; figure 1 ---	1-14
A	WO,A,94 02913 (BACON BRIAN) 3 February 1994 see claim 1; figure 1 ---	1-14
A	EP,A,0 278 740 (VERITEC INC) 17 August 1988 see claim 1; figure 1 ---	1-14
A	DE,A,33 47 607 (LAUREL BANK MACHINE CO) 12 July 1984 cited in the application see claim 1; figure 1 ---	1-14
		-/-



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

3

Date of the actual completion of the international search

29 July 1996

Date of mailing of the international search report

06.08.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Authorized officer

Kirsten, K

## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/EP 96/01178

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE,C,27 60 453 (GAO) 27 June 1991 cited in the application see claim 1; figure 1 -----	1-14

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International Application No  
PCT/EP 96/01178

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-4358849	09-11-82	FR-A-	2382724	29-09-78
		DE-A-	2809341	07-09-78
		GB-A-	1597043	03-09-81
		JP-A-	53110344	27-09-78
		SE-B-	444997	20-05-86
		SE-A-	7802443	05-09-78
-----	-----	-----	-----	-----
WO-A-9402913	03-02-94	AU-B-	4714193	14-02-94
		CN-A-	1087735	08-06-94
		EP-A-	0670071	06-09-95
		JP-T-	8502135	05-03-96
		US-A-	5495531	27-02-96
		ZA-A-	9306670	10-04-95
-----	-----	-----	-----	-----
EP-A-0278740	17-08-88	AU-B-	615174	26-09-91
		AU-B-	1161688	11-08-88
		CA-A-	1293805	31-12-91
		JP-A-	63278190	15-11-88
		US-A-	4972475	20-11-90
-----	-----	-----	-----	-----
DE-A-3347607	12-07-84	JP-C-	1737265	26-02-93
		JP-B-	4020231	02-04-92
		JP-A-	59127186	21-07-84
		GB-A,B	2133542	25-07-84
		US-A-	4539702	03-09-85
-----	-----	-----	-----	-----
DE-C-2760453	27-06-91	DE-C-	2760166	17-11-88
-----	-----	-----	-----	-----

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen  
PCT/EP 96/01178

## A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 G07D7/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprässtoff (Klassifikationssystem und Klassifikationsymbole)

IPK 6 G07D

Recherchierte aber nicht zum Mindestprässtoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US,A,4 358 849 (SERY JACQUES) 9.November 1982 siehe Anspruch 1; Abbildung 1 ---	1-14
A	WO,A,94 02913 (BACON BRIAN) 3.Februar 1994 siehe Anspruch 1; Abbildung 1 ---	1-14
A	EP,A,0 278 740 (VERITEC INC) 17.August 1988 siehe Anspruch 1; Abbildung 1 ---	1-14
A	DE,A,33 47 607 (LAUREL BANK MACHINE CO) 12.Juli 1984 in der Anmeldung erwähnt siehe Anspruch 1; Abbildung 1 ---	1-14
		-/-



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erforderlicher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

3

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

29.Juli 1996

06.08.96

Name und Postanschrift der Internationale Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Bevollmächtigter Bediensteter

Kirsten, K

## INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 96/01178

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE,C,27 60 453 (GA0) 27.Juni 1991 in der Anmeldung erwähnt siehe Anspruch 1; Abbildung 1 -----	1-14

3

**INTERNATIONALER RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 96/01178

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US-A-4358849	09-11-82	FR-A- 2382724 DE-A- 2809341 GB-A- 1597043 JP-A- 53110344 SE-B- 444997 SE-A- 7802443	29-09-78 07-09-78 03-09-81 27-09-78 20-05-86 05-09-78
-----			
WO-A-9402913	03-02-94	AU-B- 4714193 CN-A- 1087735 EP-A- 0670071 JP-T- 8502135 US-A- 5495531 ZA-A- 9306670	14-02-94 08-06-94 06-09-95 05-03-96 27-02-96 10-04-95
-----			
EP-A-0278740	17-08-88	AU-B- 615174 AU-B- 1161688 CA-A- 1293805 JP-A- 63278190 US-A- 4972475	26-09-91 11-08-88 31-12-91 15-11-88 20-11-90
-----			
DE-A-3347607	12-07-84	JP-C- 1737265 JP-B- 4020231 JP-A- 59127186 GB-A,B 2133542 US-A- 4539702	26-02-93 02-04-92 21-07-84 25-07-84 03-09-85
-----			
DE-C-2760453	27-06-91	DE-C- 2760166	17-11-88
-----			